

Marvell Driver Null SSID Association Request Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-09/msg00049.html>

- *From:* Laurent Butti <laurent.butti@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 04 Sep 2008 10:46:01 +0200
-

Title:

* Marvell Driver Null SSID Association Request Vulnerability

Summary:

* The wireless drivers in some Wi-Fi access points (such as the MARVELL-based Netgear WN802T) do not correctly parse SSID information element included in association requests. Most information elements are used by the wireless access point and clients to advertise their capabilities (regarding rates, network name, cryptographic capabilities...). More precisely, the SSID is used by the access point to validate that the wireless client intends to connect to the appropriate SSID.

Assigned CVE:

* CVE-2008-1197

Details:

* The bug can be triggered by a malicious association request to the wireless access point with a Null SSID. This can be achieved only after a successful 802.11 authentication (in "Open" or "Shared" mode according to the configuration of the wireless access point).

Attack Impact:

* Denial-of-service (reboot or hang-up) and possibly remote arbitrary code execution

Attack Vector:

* Unauthenticated wireless device

Timeline:

* 2008-02-19 - Vulnerability reported Netgear

Marvell Driver Null SSID Association Request Vulnerability

- * 2008-03-06 – PoC sent to Netgear
- * 2008-09-04 – Public disclosure

Affected Products:

- * Netgear WN802T (firmware 1.3.16) with MARVELL 88W8361P-BEM1 chipset

Vulnerable Devices:

* As it is a wireless driver specific issue, the wireless vendor should use the latest chipset wireless driver for their access point firmwares. This security vulnerability was reported to Netgear, updated firmwares should be available on their web site. Any other wireless device relying on this vulnerable wireless driver is likely to be vulnerable.

Credits:

* This vulnerability was discovered by Laurent Butti and Julien Tinnes from France Telecom / Orange